Health Data Security:
Go Deep, Go All-Out

Holistic security programs include physical, network and application safeguards

Widespread adoption of electronic health records and the growing use of software applications have made electronic data a key factor in the care-delivery process, and one that is often heralded for its potential to improve outcomes and reduce costs. As a result, the healthcare industry has finally recognized the value of digital data. The flip side: Others have realized the value of this data as well, and that's why it is often in a precarious state.

While healthcare organizations are tapping into the myriad benefits associated with electronic data, they are also facing the realities associated with data risk like never before. The numbers, in fact, are startling. Healthcare data breaches grew from about 2.7 million in 2012, to 6.9 million in 2013, to 12.5 million in 2014, to more than 94 million through the first half of 2015, according to the U.S. Department of Health and Human Services. Some organizations have been hit hard, with 80 million people affected by a hacking incident at one healthcare organization and 11 million affected by an incident at another.[1]

The best defense? One that runs ocean-like deep. "Healthcare organizations need to have multiple layers of defense. These layers should include everything from awareness to policy to physical safeguards to network and server security to application security," said Chris Bowen, chief privacy and security officer and founder at ClearDATA. "Each of these layers is very important; because if you leave any of these without the proper hardening, then you will have glaring holes in your defense strategy."

What's more, safeguarding protected health information (PHI) requires a dynamic process capable of meeting changing requirements. For example, the ability to pivot is required to meet the needs associated with a continually evolving "technology stack," which in recent years has grown to include a variety of form factors such as tablets; various architectural options such as cloud technology; and a plethora of mobile apps used by professionals and patients alike.

Produced in partnership with
HIMSS Media

"Healthcare organizations need to have multiple layers of defense."

— **Chris Bowen** | Founder, Chief Privacy & Security Officer | ClearDATA

"In healthcare, you have silos – and silos within silos. So, you need to facilitate holistic communication around the entire security solution," Bowen said. "If you don't, you might get an infrastructure team that's separated from the application team. So, you might have one level of defense that is bolstered but another that may have been forgotten. Without having it all hardened in a way that's effective, you are likely to have a problem."

Parts of the whole

When considering holistic security, healthcare organizations need to address a variety of factors including:

Physical safeguards. Physical threats are a growing concern. When assessing a data center, leaders need to understand both what they are up against and what is being done to mitigate risk.

"You have to understand the physical safeguards that the data center has in place to protect against natural disasters, which seem to be more prevalent in recent years, or any type of malicious insider activity," said Lee Kim, JD, director, privacy and security, HIMSS North America. As such, leaders need to make sure that data centers can protect data against any potentially disruptive event. Some centers, according to Lee, ensure physical security with:

- Foot-wide concrete walls on all sides of the building to protect against natural disasters
- Video surveillance to monitor who is gaining entrance to the facility
- Armed security guards to prevent intruders from entering the facility
- Multi-factor authentication (i.e., identification card and palm reader) to gain access
- Zoned access, making it possible for staff to only gain entrance to areas where specific equipment is located

Network/Server Security. Network/server security threats are also on the rise. As such, healthcare organizations need to engage in best practices to secure data.

When assessing network/server security, the server design should be closely scrutinized. "If you are going to implement an application that is processing PHI, is it a good idea to place that information on a server that is accessible from the public Internet? No, heavens, no," Bowen said. "Instead, servers should be architected in a way that supports the class of data that they are working with. So, PHI should be stored on a server inside a secure zone with very limited traffic. The architecture should protect and isolate the data."

"You have to understand the physical safeguards that the data center has in place to protect against natural disasters, or any type of malicious insider activity."

— **Lee Kim, JD** | Director, Privacy & Security | HIMSS North America

It is also important to back up data in a variety of ways. "Organizations should use a combination of local and remote backups," Lee said. "You may also want to use a combination of a full backup with incremental or differential backups. By the same token, you may also want to perform a full backup on a weekly basis, but an incremental or a differential backup every day."

In addition, when working with a third party to provide network services, healthcare organization leaders need to not only ensure that they have a business associate agreement in place, as required by HIPAA, they also should perform some "due diligence" to ensure that security is optimal.

"Healthcare organizations need to look closely at how third parties are handing security because at the end of the day, if you've got Fort Knox-like security at your organization and [your third-party provider] is leaving the key in the door, it's going to come back to haunt you," said Adam Greene, JD, partner and co-chair of the Health Information Practice at Davis Wright Tremaine, a national law firm with offices across the country.

While HIPAA does not specifically demand healthcare organizations to perform this "due diligence" with respect to the security practices of business associates, healthcare organizations should move beyond baseline requirements and assess third-party security practices through a questionnaire or an onsite audit.

"Even though you won't be held to a HIPAA violation if you don't do the due diligence, you could experience a breach that will result in harm to your organization's reputation or financial situation," Greene said.

Application Security. Application security has become more important in recent years as the volume of healthcare-related apps has grown exponentially. "With so many applications on mobile devices like iPads and iPhones and Android devices, you have a lot more entrance into the market from a software perspective," Bowen said. What's more, in the rush to market these apps, security concerns are sometimes relegated to the backburner.

Apps, however, should be thoroughly vetted before being utilized. "Secure coding practices need to be part of the software development cycle," Bowen said. "Applications need to have proper code reviews from third parties that really expose any vulnerabilities or weaknesses. And if you have experts helping you along the way from an architecture perspective and a hardening perspective, that bolsters your chances of keeping your data safe."

"Even though you won't be held to a HIPAA violation if you don't do the due diligence, you could experience a breach that will result in harm to your organization's reputation or financial situation."

— **Adam Greene, JD** | Partner & Co-chair, Health Information Practice | Davis Wright Tremaine

A formal security check should be standard operating procedure before utilizing any app. For example, if an organization plans to use a web app to present patient data, leaders should determine the safest language to deploy the app in; decide where the app can be hosted most securely; assess how vulnerable the app is to unauthorized access; understand the ramifications associated with any unauthorized access; and develop safeguards that prevent password sharing.

Perhaps most importantly, though, the code should be scanned to ensure that potential vulnerabilities have not been overlooked. "We recently ran a scan on an application that's in use in the life sciences, and lo and behold, we found a hardcoded password in the code itself," Bowen said. "It's human nature to forget or to miss something. That's why you need to checks and balances or some oversight in place."

Indeed, a comprehensive approach to data security is a non-negotiable in today's healthcare environment. By taking a holistic approach to data security, healthcare organizations can tap into the benefits associated with electronic data, while reducing the risks.

References

[1] Breach Portal. U.S. Department of Health and Human Services. Accessed at: https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf